

## CLAIMS

1. An information processing device for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information, the device comprising:

decoding means for decoding the first key with the second key; and

request means for requesting transmission of the second key when the decoding means cannot decode the first key.

2. An information processing method for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information, the method comprising:

a decoding step of decoding the first key with the second key; and

a request step of requesting transmission of the second key when the first key cannot be decoded at the decoding step.

3. A program providing medium for providing a computer-readable program which causes an information processing device for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information, to execute processing comprising:

a decoding step of decoding the first key with the second key; and

a request step of requesting transmission of the second key when the first key cannot be decoded at the decoding step.

4. An information processing device for receiving encrypted information, an

accounting means for executing processing for accounting; and

5. An information processing method for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information, the method comprising:

a request step of requesting transmission of the second key when an accounting value at the accounting step has reached a predetermined value.

an accounting step of executing processing for accounting; and

7. An information processing device for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the

storage means for storing data specifying the information processing device;  
transmission means for transmitting the data specifying the information processing device to the management device; and

8. An information processing method for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key from a system managed by a predetermined management device so as to decode the information, the method comprising:

a storage step of storing data specifying an information processing device;  
a transmission step of transmitting the data specifying the information processing device to the management device; and

9. A program providing medium for providing a computer-readable program which causes an information processing device for receiving encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key from a system managed by a predetermined management device so as to decode the information, to execute processing comprising:

a transmission step of transmitting the data specifying the information

... a request step of requesting transmission of the second key when the data specifying the information processing device is transmitted.

the first storage means comprising first mutual authentication means for carrying out mutual authentication with the first decoding means and generating a temporary key, second storage means for storing the second key, second decoding means for decoding the first key with the second key, and encryption means for encrypting the first key with the temporary key,

11. An information processing method for an information processing device having storage means and decoding means for using encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to

the storage means including a first mutual authentication step of carrying out mutual authentication with the decoding means and for generating a temporary key,

a first decoding step of decoding the first key with the second key, and

the decoding means including a second mutual authentication step of carrying out mutual authentication with the first storage means and for generating a temporary

a second decoding step of decoding the first key with the temporary key, and

12. A program providing medium for providing a computer-readable program with respect to an information processing device having storage means and decoding means for using encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information,

a first mutual authentication step of carrying out mutual authentication with the  
ing means and for generating a temporary key;

a first decoding step of decoding the first key with the second key; and

an encryption step of encrypting the first key with the temporary key;

the program causing the decoding means to execute processing comprising:  
 a second mutual authentication step of carrying out mutual authentication with  
 the first storage means and for generating a temporary key;  
 a second decoding step of decoding the first key with the temporary key; and  
 a third decoding step of decoding the information with the first key.

13. An information providing system comprising an information providing device  
 for providing encrypted information, an information distribution device for distributing  
 the provided information, an information processing device for decoding and using the  
 distributed information, and a management device for managing the information  
 providing device, the information distribution device and the information processing  
 device,

the information providing device having first transmission means for appending  
 information indicating the handling of information to the encrypted information and  
 for transmitting the resultant information to the information distribution device,

the information distribution device having calculation means for calculating the  
 use fee of the information on the basis of the information indicating the handling of  
 the information transmitted from the information providing device, and second  
 transmission means for appending the use fee to the encrypted information and for  
 transmitting the resultant information to the information processing device,

the information processing device having accounting information preparation  
 means for preparing accounting information corresponding to the use of the

the management device having detection means for detecting an unauthorized action from a part of or all of the accounting information, the information indicating the handling of information and the use fee.

15. The information providing system as claimed in claim 13, wherein the accounting information and the information indicating the handling of information are encrypted and then transmitted.

the information providing method for the information providing device including a first transmission step of appending information indicating the handling of information to the encrypted information and transmitting the resultant information to

the information providing method for the information distribution device including a calculation step of calculating the use fee of the information on the basis of the information indicating the handling of the information transmitted from the information providing device, and

the information providing method for the information processing device including an accounting information preparation step of preparing accounting information **corresponding** to the use of the information on the basis of the use fee, and

the information providing method for the management device including a detection step of detecting an unauthorized action from a part of or all of the accounting information, the information indicating the handling of information and the use fee.

17. A program providing medium for providing a computer-readable program with respect to an information providing system comprising an information providing device for providing encrypted information, an information distribution device for





the program causing the management device to execute processing including a detection step of detecting an unauthorized action from a part of or all of the accounting information, the information indicating the handling of information and the use fee.

18. An information providing system comprising an information providing device for providing encrypted information, an information distribution device for distributing the provided information, an information processing device for decoding and using the distributed information, and a management device for managing the information providing device, the information distribution device and the information processing device,

the information providing device having first transmission means for appending information indicating the handling of information to the encrypted information and then transmitting the resultant information to the information distribution device,

the information distribution device having second transmission means for transmitting the encrypted information received from the information providing device and the information indicating the handling of information to the information processing device,

the information processing device having use permission information preparation means for preparing use permission information corresponding to the use of the information on the basis of the information indicating the handling of information, and third transmission means for transmitting the use permission

information together with a part of or all of the information indicating the handling of information to the management device,

the management device having detection means for detecting an unauthorized action from a part of or all of the use permission information and the information indicating the handling of information.

19. The information providing system as claimed in claim 18, wherein the use permission information and the information indicating the handling of information are signed and then transmitted.

20. The information providing system as claimed in claim 18, wherein the use permission information and the information indicating the handling of information are encrypted and then transmitted.

21. An information providing method for an information providing system comprising an information providing device for providing encrypted information, an information distribution device for distributing the provided information, an information processing device for decoding and using the distributed information, and a management device for managing the information providing device, the information distribution device and the information processing device,

the information providing method for the information providing device including a first transmission step of appending information indicating the handling of information to the encrypted information and then transmitting the resultant information to the information distribution device,

20250303 15:55:50





registration means having ID of the information processing device and data indicating the availability of registration with respect to that ID, for registering the information processing device on the basis of the ID of the information processing device.

24. The management device as claimed in claim 23, wherein the data includes data indicating the possibility of settlement corresponding to the ID.

25. The management device as claimed in claim 23, wherein the registration means registers another information management device subordinate to the information management device communicating with the management device.

26. A management method for managing an information providing device for providing encrypted information and an information processing device for using the information, the management method comprising

a registration step of having ID of the information processing device and data indicating the availability of registration with respect to that ID and registering the information processing device on the basis of the ID of the information processing device.

27. A program providing medium for providing a computer-readable program which causes a management device for managing an information providing device for providing encrypted information and an information processing device for using the information, to execute processing including

a registration step of having ID of the information processing device and data



processing device subordinate to the information processing device.

32. An information utilization system comprising an information processing device for decoding information encrypted and provided thereto and a management device for managing the information processing device,

the management device having registration means having ID of the information processing device and data indicating availability of registration with respect to that ID for registering the information processing device on the basis of the ID of the information processing device,

the information processing device having registration request means for requesting registration of another information processing device subordinate to the information processing device.

33. An information processing device which is managed by a management device and is connected to another information processing device and which decodes and uses encrypted information, the information processing device comprising:

mutual authentication means for carrying out mutual authentication with the management device and said another information processing device;

decoding means for decoding predetermined information;

transmission/reception means for transmitting/receiving a registration condition prepared by the management device;

storage means for storing the registration condition transmitted/received by the transmission/reception means; and



control means for controlling the operation on the basis of the registration condition stored by the storage means.

34. An information processing method for an information processing device which is managed by a management device and is connected to another information processing device and which decodes and uses encrypted information, the method comprising:

a mutual authentication step of carrying out mutual authentication with the management device and said another information processing device;

a decoding step of decoding predetermined information;

a transmission/reception step of transmitting/receiving a registration condition prepared by the management device;

a storage step of storing the registration condition transmitted/received at the transmission/reception step; and

a control step of controlling the operation on the basis of the registration condition stored at the storage step.

35. A program providing medium for providing a computer-readable program which causes an information processing device which is managed by a management device and is connected to another information processing device and which decodes and uses encrypted information, to execute processing comprising:

a mutual authentication step of carrying out mutual authentication with the management device and said another information processing device;

a decoding step of decoding predetermined information;

a transmission/reception step of transmitting/receiving a registration condition prepared by the management device;

a storage step of storing the registration condition transmitted/received at the transmission/reception step; and

a control step of controlling the operation on the basis of the registration condition stored at the storage step.

36. A management device for managing an information processing device which decodes and uses encrypted information, the management device comprising:

encryption means for encrypting data to be supplied to the information processing device;

execution means for executing predetermined processing when a registration condition is transmitted from the information processing device;

preparation means for preparing the registration condition of the information processing device when executing the predetermined processing by the execution means; and

transmission means for transmitting the registration condition prepared by the preparation means to the information processing device.

37. A management method for a management device for managing an information processing device which decodes and uses encrypted information, the method comprising:



39. An information processing device for decoding and using encrypted information, the device comprising:

permission information generation means for generating information indicating a permission condition for the use of the information;

authentication information generation means for generating authentication information of the information indicating the permission condition; and

storage means for storing the authentication information.

40. The information processing device as claimed in claim 39, wherein the storage means has a tamper-resistant structure.

41. An information processing method for decoding and using encrypted information, the method comprising:

a permission information generation step of generating information indicating a permission condition for the use of the information;

an authentication information generation step of generating authentication information of the information indicating the permission condition; and

a storage step of storing the authentication information.

42. A program providing medium for providing a computer-readable program which causes an information processing device for decoding and using encrypted information to execute processing comprising:

a permission information generation step of generating information indicating a permission condition for the use of the information;

09561533-550700  
007099-550700











a storage step of storing data specifying the information and data indicating an amount to be paid to the information provider for the use of the information;

a settlement instruction step of instructing a settlement institution to settle an account for each information provider on the basis of the profit of each information provider.

a storage step of storing data specifying the information and data indicating an amount to be paid to the information provider for the use of the information;

a settlement instruction step of instructing a settlement institution to settle an account for each information provider on the basis of the profit of each information provider.

59. An information processing device for storing predetermined information to an external storage medium loaded therein, and for decoding encrypted information and using the decoded information, the device comprising:

encryption means for encrypting predetermined information with a predetermined key.

60. The information processing device as claimed in claim 59, wherein the predetermined key is a public key of a management device managing the information processing device.

61. An information processing method for an information processing device for storing predetermined information to an external storage medium loaded therein, and for decoding encrypted information and using the decoded information, the method comprising:

· a mutual authentication step of carrying out mutual authentication with the external storage medium loaded therein; and

an encryption step of encrypting predetermined information with a predetermined key.

62. A program providing medium for providing a computer-readable program which causes an information processing device for storing predetermined information to an external storage medium loaded therein and for decoding encrypted information and

a mutual authentication step of carrying out mutual authentication with the external storage medium loaded therein; and

63. A management device for managing an information processing device for decoding and using encrypted information, the management device comprising

64. A management method for managing an information processing device for decoding and using encrypted information, the method comprising

65. A program providing medium for providing a computer-readable program which causes a management device for managing an information processing device for decoding and using encrypted information to execute processing comprising

66. An information utilization system comprising an information processing device for storing predetermined information to an external storage medium loaded thereon and for decoding and using encrypted information, and a management device for

the information processing device having mutual authentication means for carrying out mutual authentication with the external storage medium loaded thereon, and encryption means for encrypting predetermined information with a public key of the management device,

67. An external storage medium loaded on an information processing device for decoding and using encrypted information, the external storage medium comprising mutual authentication means for carrying out mutual authentication with the information processing device.